Volume 13, Issue 10   Atari Online News, Etc.   March 11, 2010

Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1310   03/11/10

~ Sony Gets Geohot Logs! ~ Panel To Examine Google ~ Five Pac-Man Unknowns!

-* Law Could Damage Online Rights *-

-* Five Big Security Threats for 2011! *-

-* China’s Cyber Abilities Worries the States *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"

""""""""""""""""""""""""""

The horrendous winter that we’ve experienced here in New England and many other parts of the country pales in comparison to what Japan has just experienced, as well as those in Hawaii and the U.S. west coast. It’s bad enough to have an earthquake, but one of the magnitude that Japan has just experienced is mind-boggling. And to top that off, the after-effect was a huge tsunami - so huge that it managed to get to Hawaii and the west coast of the U.S. and cause significant damage and loss of life!

And this weather "event" is just another of numerous natural disasters that have occurred recently - tornadoes in the South, another major quake in New Zealand, and many others. Mother Nature has certainly been in a bad mood lately, for lack of a better non-sexist description. I can’t imagine what other parts of the world are experiencing, but terror would be one way to describe it!

Things here in the Northeast have eased up a bit. Yes, we’ve been getting rain and some flooding, but nothing compared [yet] to what we experienced last year. The snow is melting quickly; and I can actually see numerous patches of my lawn throughout the yard. Maybe, hopefully, Spring is finally starting to make its way to our area. One other sure sign of better things to come - don’t forget to set your clocks AHEAD one hour this weekend for Daylight Savings Time. Sure, it’s another hour of lost sleep, but this one I can manage to appreciate somehow!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Judge Hands Over Geohot Sites IP Logs to Sony
!

""""""""""""""""""""""""""""" Five Things You Never Knew About Pac-Man!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Judge Hands Over IP Logs of Several Geohot Sites to Sony

IconEver visited the website of famed iOS and Playstation 3 hacker Geohot? Or watched his video on YouTube? Or read his Blogspot blog? Well, you’re now part of a criminal investigation. A US judge has given Sony complete and unrestricted access to all IP addresses which ever visited his website and blog, or watched his YouTube video.

There’s two reasons why Sony wants all this information. First, Sony wants to demonstrate that Geohot’s Playstation 3 code was distributed widely. Second, Sony wants to show that enough Californians downloaded the code, making it acceptable for the case to take place in San Francisco, instead of Geohot’s home state New Jersey.

Magistrate Joseph Spero has ordered Google to hand over all server and IP logs for Geohot’s Blogspot blog. BlueHost, which hosts Geohot’s website, is also forced to hand over all server and IP logs. As for YouTube - they must hand over all account information related to an account named "geohot", as well as all possible identifying information related to all the people who watched or commented on a video posted by this account. Twitter must hand over all tweets, personal messages, and account information.

That’s a whole boatload of information. Considering we and lots of other websites linked to his website quite a few times, I’m pretty sure many of you are now part of a criminal investigation. It’s absolutely beyond me how any judge with more than two braincells can disregard privacy concerns this easily. It’s very hard to maintain that this judge is impartial. I’ve never had a whole lot of faith in the US justice system whenever large companies were involved, and things like this do little to restore my faith.

Sony has threatened to sue anyone who posts the encryption key or hosts the jailbreak tools. Normally, I would post the key right here, since those silly pro-corporation laws the US is so fond of do not apply in Europe. Sadly, OSNews is a US site hosted in the US, so I can’t take that risk.

=~=~=~=

->A-ONE Gaming Online   -   Online Users Growl & Purr!
"""""""""""""""""""

Five Things You Never Knew About Pac-Man

Pac-Man Having been a part of the pop-culture landscape for over 30 years now, Pac-Man is a pretty familiar character.

He has adorned cereal boxes, been the star of a Saturday morning cartoon program and appeared on virtually every gaming platform to have ever been released.

That’s not just systems from Microsoft, Sony and Nintendo. It also includes essentially every cell phone that has a screen, long-dead portable systems and plug-and-play devices for your TV. Along the way, the little pellet-muncher has built an empire that has allowed publisher Namco-Bandai to survive the worst the economy could throw at it.

But even the most well known icons have their secrets. This week, at the Game Developers Conference in San Francisco, Toru Iwatani, creator of the game, offered a postmortem on the industry’s biggest franchise-and told a few tales most fans have probably never heard.

Here are the five most surprising:

The point of the game was to attract girls

While today’s player is slightly more likely to be male, gaming in the late 1970s was pretty much exclusively a men’s club. Iwatani wanted to change this, creating something that could appeal to both women and families, he says.

"The reason I created Pac-Man was because we wanted to attract female gamers," he says. "Back then, there were no home games. People had to go to the arcade center to play games. That was a playground for boys. It was dirty and smelly. So we wanted to include female players, so it would become cleaner and brighter."

Each ghost had specific orders

When you play the game, it might seem as if the four ghosts are actively chasing you. That’s not exactly true. Iwatani intentionally avoided programming them with that purpose, since that would have resulted in Pac-Man zipping around the screen with four ghosts always right behind him.

Instead, it’s only Blinky, the red ghost, who doggedly pursues you throughout the game. Pinky, the pink ghost (naturally), simply wants to position itself at a point that’s 32 pixels in front of Pac-Man’s mouth. The blue ghost, Inky, is seeking to position itself at a similar fixed spot. And Clyde, the orange ghost, moves completely at random.

Because the player constantly has Pac-Man on the go, however, the ghosts are always changing direction and trying to achieve their goal, which adds to the challenge of the game.

What, exactly, does Pac-Man mean?

You may have heard the story about how a pizza with a missing slice inspired Pac-Man’s design. But it turns out the game was designed entirely around food.

"I thought about something that may attract girls," says Iwatani. "Maybe boy stories or something to do with fashion. However, girls love to eat desserts. My wife often does! So the verb eat’ gave me a hint to create this game."

That theme continued with the game’s name. In Japanese, "puck puck" is akin to the U.S. saying "munch munch". So the original name - Puck-Man - translated as "Munch man". (A savvy Midway Games official changed it to Pac-Man when the game hit the U.S. to discourage vandals from shaving off part of the "P," thereby creating an obscene word.)

The missing puzzle piece

Pac-Man was designed to be as simple as possible, to attract a wide audience. The limits of technology in 1980 made this a little easier to achieve. Iwatani says he’s happy about this now, but at the time, there was one more thing he wanted to add to the game.

"I wanted to have a shelter and it would move up and down," he says. "When the ghost comes, the ghost would be pinched by the shelter which would disfigure the ghost."

The ghosts were almost just one color

It’s kind of hard to picture Pac-Man without the brightly colored ghosts today, but when the game was being developed, Iwatani says he was pressured hard to change that.

The president of Namco ordered him to make the ghosts a single color - red, to be precise - since she believed players would be confused that some ghosts, perhaps, were Pac-Man’s ally.

Iwatani refused the order and on questionnaires to the game’s testers, asked if they would prefer a single color ghost or four. Not a single person wanted the single-color option. That ultimately convinced the president she was wrong.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

New EU Consumer Law Could Damage Online Rights, BSA Claims

Including digital content and services in the new Consumer Rights Directive could have a detrimental effect on online consumers, the Business Software Alliance (BSA) said on Monday.

The organization, which represents such software giants as Microsoft, SAP, IBM, Dell and HP, has hit out at the controversial legislation, which is aimed at revising European customer protection on national and cross-border contracts.

To date, the proposed text of the directive has faced criticism from consumer groups for failing to take sufficient account of consumer rights for online digital purchases such as music, video, books and software. However the BSA argues that the Consumer Rights Directive is simply not the right vehicle for enhancing consumer protection of digital products at all.

Customers could find themselves trying to resolve failed downloads with their internet service provider rather than the trader, the BSA claims. It also alleges that traders could stop offering patches and updates because they are only liable for faults at the time of purchase.

Preliminary agreement on the draft directive was reached last month between the European Commission and member states. However, the European Parliament must approve the text before any law can be implemented.

DigitalEurope and the European Digital Media Association have also expressed concern and are developing a joint letter with the BSA to be submitted to MEPs urging them to oppose the inclusion of digital products as part of the sale of goods provisions in the proposed directive.

The current text has so far only been approved at committee level. The Internal Market and Consumer Protection committee voted narrowly to approve the revised text on Feb. 1. But members agreed that further discussion would be necessary to "futureproof" any directive.

Currently there is a 14-day "cooling off" period during which consumers can withdraw from a contract. The revised directive proposes a standard withdrawal form to make it easier for consumers to pull out of a contract. It also envisages a ban on all pre-ticked boxes which apply to payments, such as for express delivery in distance selling or travel insurance, priority boarding and baggage when booking a holiday. Consumers will have the right to be reimbursed the extra payments to which they have not actively agreed.

"Digital content transmitted to the consumer in a digital format, where the consumer obtains the possibility of use on a permanent basis or in a way similar to the physical possession of a good, should be treated as goods for the application of the provisions of this Directive which apply to sales contracts. However, a withdrawal right should only apply until the moment the consumer starts to download the digital content," says the current draft.

The text will be put to a full parliament vote on 24 March, but some political groups already look likely to reject it.

Five Big Security Threats for 2011

Online malicious activity was a major headache in 2010, and so far, 2011 is no different: We’ve seen scams and malware on Twitter, Facebook, and the Android Market, as well as a rise in politically motivated online attacks.

But that’s no surprise to security experts such as Graham Cluley, senior technology consultant for security firm Sophos. Cluley says that Sophos analyzes about 95,000 pieces of malware every day that is either brand-new or a variant of an older attack.

The bad guys are hard at work figuring out new ways to infect your system. The good news is that the latest antivirus programs do a better job than ever at detecting suspicious activity before it can damage your computer.

But security software can’t always protect you; sometimes the best defense is a dose of common sense and a little bit of knowledge about what to watch out for. Whether it’s fake antivirus scams, malware on social networks, or good old-fashioned e-mail attachments loaded with viruses, it pays to be on your toes so you don’t end up becoming a victim to identity theft, a raided bank account, or even a home invasion.

So here’s a look at 2011’s five big security threats, and the steps you can take to avoid becoming a victim.

Threat 1: Mobile Apps

*What it is: *It isn’t surprising that smartphones are a hot new malware target: 85 percent of adults in the United States own a mobile phone, according to a recent study by the Pew Internet and American Life Project, and the smartphone market is growing at a rapid pace.

As recently as March 1, more than 50 third-party applications on Google’s official Android Market contained a Trojan called DroidDream. When you run a DroidDream application for the first time, the malware gains administrator access over your phone without your permission, according to mobile security firm Lookout. That means it could download more malicious programs to your phone without your knowledge and steal data saved on your device.

Google was able to stop the DroidDream outbreak by deleting the bad apps from the Market and remotely removing malicious apps from Android users’ devices, but it’s only a matter of time before the next outbreak occurs.

And malicious apps on the Android Market aren’t the only way that malware authors can target phones: A recent Android malware outbreak in China spread through repackaged apps distributed on forums or through alternative app markets.

The threat of malware, coupled with other security threats (such as data leakage from a lost phone) may soon impact your ability to use personal devices at work, according to Andrew Jaquith, chief technology officer of Perimeter E-Security. Companies may begin to set some serious ground rules for putting company data on personal mobile devices by enforcing "policies for passwords, device locking, remote wipe, and hardware encryption," Jaquith says.

Protect yourself: You can’t trust that all apps on the Android Market are malware free. Make sure you read app reviews in the Market and on reputable app review sites such as PC World’s AppGuide. And avoid installing any applications you get from unknown sources. That .apk file may be titled "Fruit Ninja" but in reality is a Trojan horse waiting to be unleashed. Don’t forget that a number of mobile antivirus apps are available for Android, and it may be wise to have at least one installed on your phone.

Also, read an app’s permissions screen carefully - it details what kinds of data an Android application can access (Google makes it mandatory for developers to have a complete list of permissions for every feature that an app has access to on your phone). You can find this list on every app’s page in the Android Market (it appears right after you tap the button to download an app). See if you can uncheck undesirable permissions. If you’re downloading a wallpaper application, for example, chances are it doesn’t need to know your exact location.

iOS users aren’t off the hook, either: Some bad actors have slipped by Apple’s censors in the past despite the company’s third-party app-vetting process. Over the summer, for example, a flashlight app that had hidden functionality got approved to the App Store. The actual risk may be low, but it isn’t impossible for a seemingly legit app to have some hidden, malicious capabilities.

Threat 2: Social Network-Based Scams

Social networks such as Facebook and Twitter may be a great place to connect with friends, but they are also a breeding ground for malicious activity. Cluley says some of the most rapid growth in online attacks comes from social networks. In November, antivirus maker BitDefender made a similar statement, saying 20 percent of all Facebook users are active targets of malware.

Social network scams often take the form of phishing attacks that try to lure you in with photos or videos, and harvest your personal information or Facebook login - or worse, infect your PC with malware - along the way. Often, these links will come from Facebook friends who fall victim to these scams. You could also run across rogue Facebook applications that try to access your Facebook data and that of your friends.

While it’s probably no big deal if scam artists find out what your favorite movies or quotes are, your profile may contain critical data - such as your date or place of birth, cell phone number, and e-mail address - that can be used to build a profile about you and even steal your identity. Such bits of information may be the final data point a bad actor needs to impersonate you online.

You could even become a specific target for criminals through social networks. In September, three young men ran a burglary ring in Nashua, New Hampshire, by looking at Facebook postings about people going out and then targeting homes they believed were likely to be empty. Police said they recovered over $100,000 in stolen property after cracking the ring, according to New Hampshire’s WMUR-TV 9.

Protect yourself: Be wary of any social networking postings that offer you the chance to see a cool photo or video or making claims you know to be untrue - such as a recent Twitter scam that offered to let you see who is viewing your profile. Often, these scams can be stopped by just revoking the app in your security permissions and changing your account password. Another smart thing to do, according to Cluley, is to stop and ask yourself why a Facebook application wants to post messages on your wall or access your friends list. If you can’t think of a good reason the app would need to do this, perhaps it’s not worth authorizing.

Threat 3: Fake Antivirus

What it is: Although they’ve been around for a few years now, fake antivirus scams are on the rise, according to Cluley. In the last eight months, Sophos says, it has analyzed more than 850,000 instances of fake antivirus. Also known as "scareware," these scams start by convincing you to download a free antivirus program, sometimes appearing to be software from a reputable security company. Then the software claims your computer is under threat from a virus and you can save your system by buying a "full" version of the antivirus program for a one-time fee.

Once you do that, however, not only have you allowed more potential malware onto your computer, but you may have also handed over your credit card credentials to identity thieves. At that point, the bad guys can drain your bank account or steal your identity.

The irony of all this, says Cluley, is that these scams owe some of their success to the fact that we are becoming more aware of computer security. Since we want to protect ourselves as much as possible from malware threats, we become easily seduced by software promising enhanced security.

Protect yourself: First and foremost, make sure you are running a security program that’s current - especially one that effectively blocks brand-new malware (see our reviews of the latest security suites and antivirus programs for which to buy). And never download a security program from a pop-up window you see online or from a third-party site.

Threat 4: PDFs

It may be the oldest online scam in the book, but e-mail loaded with malware attachments is still a big problem despite a high degree of awareness and robust antivirus scanning in Webmail clients such as Gmail and Yahoo Mail. Cluley puts the number of malware-related e-mails sent every day in the "millions," and says that "more and more spam is less about touting Viagra or fake degrees, but [is] turning malicious in nature."

PDF documents appear to be a prime method for these attacks, according to a recent report by MessageLabs, a division of Symantec. "PDFs are potentially one of the most dangerous file formats available and should be treated with caution...Because it is significantly easier to generate legitimate and concealed malicious content with PDFs," MessageLabs said in its February 2011 Intelligence Report (a PDF link - oh, the irony).

In 2010, 65 percent of targeted e-mail attacks used PDFs containing malware, up from 52.6 percent in 2009, according to MessageLabs, which further predicts that by mid-2011, 76 percent of targeted malware attacks could be using PDFs as their primary method of intrusion.

It’s not just businesses that are targets of e-mail scams either. Sophos recently discovered an e-mail scam in the U.K. purporting to offer an $80 gift certificate to customers of a popular pet supply retailer.

Protect yourself: Make sure you are running an antivirus program and that it’s up-to-date. Also, never open an e-mail attachment that you weren’t expecting.

Last but not least, make sure that you keep Adobe Reader (or the PDF reader of your choice) up-to-date; Adobe regularly releases security updates that fix known flaws. The new Adobe Reader X has an updated security architecture that can better protect you against malicious PDF attacks.

Threat 5: War Games

State-sponsored malware attacks, industrial espionage, and hacktivism are on the rise, according to Perimeter E-Security’s Jaquith. They may not be threats that affect everyone, but if you manage security for a business, they are the sorts of issues you should be paying attention to.

The hacktivist group Anonymous, for example, grabbed headlines this year for mounting attacks in defense of whistle-blower site WikiLeaks, and attacking government Websites in support of recent protests in Egypt, Tunisia, and Libya. The group also leaked a cache of e-mail messages from a security researcher who was trying to identify Anonymous members. "Whether it’s WikiLeaks, Anonymous, or a Chinese or Russian attacker, theft of industrial secrets is shaping up to be one of the key issues of 2011," Jaquith says in a statement.

*Protect yourself: *If you are trying to safeguard your company’s secrets or are worried about data leaks, monitor your company’s network traffic for suspicious activity and conduct regular reviews of employee data access privileges.

The Internet may be filled with malware and potential threats, but that doesn’t mean you need to panic. Keep your guard up, use common sense, and keep your software up-to-date, and you should be able to reduce your risk of falling victim to attack.

China’s Cyber Abilities Worry U.S.

China’s growing capabilities in cyber-warfare and intelligence gathering are a "formidable concern" to the United States, the top intelligence official told a Senate panel on Thursday.

"The Chinese have made a substantial investment in this area, they have a very large organization devoted to it and they’re pretty aggressive," Director of National Intelligence James Clapper told the Senate Armed Services Committee.

"This is just another way in which they glean information about us and collect on us for technology purposes, so it’s a very formidable concern," he said.

Clapper, addressing questions at an annual hearing on worldwide security threats, did not elaborate on Chinese cyber activities.

But in his written testimony, the intelligence chief said 2010 saw a "dramatic increase in malicious cyber-activity targeting U.S. computers and networks." The passage did not specifically mention China.

Clapper also cited an April 8, 2010, incident in which state-owned China Telecom advertised erroneous network routes that instructed "massive volumes" of U.S. and other foreign Internet traffic to go through Chinese servers for 17 minutes.

"This incident affected traffic to and from U.S. government and military sites, including sites for the Senate, the Army, the Navy, the Marine corps, the air force, and the office of the Secretary of Defense, as well as a number of Fortune 500 firms," he said.

When that incident was revealed in late 2010, China Telecom denied that it hijacked U.S. Internet traffic. China’s standard response to cyber-attack allegations has been to deny any connection to them and say it is also a victim of such attacks.

US Warns of Quake-Related Internet Scams

US computer security authorities warned on Friday that online scammers may seek to exploit the earthquake in Japan.

The US Computer Emergency Readiness Team (US-CERT) told computer users to be wary of "potential email scams, fake antivirus and phishing attacks regarding the Japan earthquake and the tsunami disasters."

"Email scams may contain links or attachments which may direct users to phishing or malware-laden websites," US-CERT said in a statement.

"Fake antivirus attacks may come in the form of pop-ups which flash security warnings and ask the user for credit card information," it said.

"Phishing emails and websites requesting donations for bogus charitable organizations commonly appear after these types of natural disasters," US-CERT added.

Phishing refers to attempts to steal user names, passwords and other personal information from unsuspecting victims, mostly through email or instant messages.

The massive, 8.9-magnitude quake left hundreds dead in Japan and unleashed a tsunami in the Pacific.

Senate Panel To Look into Google and Web Search

The US senator who chairs the subcommittee on anti-trust issues has announced plans to examine Google’s "dominance" of the Internet search market.

Herb Kohl, a Democrat from Wisconsin who chairs the Senate Judiciary Committee’s Subcommittee on Antitrust, Competition Policy, and Consumer Rights, put online search on the agenda for the new session of Congress.

Kohl said the subcommittee planned to address competition in online markets and Internet search issues.

"Access to the wealth of information and e-commerce on the Internet is essential for consumers and business alike," the senator said in a statement.

"The subcommittee will strive to ensure that this sector remains competitive, that Internet search is fair to its users and customers, advertisers have sufficient choices, and that consumers’ privacy is guarded.

"In recent years, the dominance over Internet search of the world’s largest search engine, Google, has increased and Google has increasingly sought to acquire e-commerce sites in myriad businesses," Kohl said.

"In this regard, we will closely examine allegations raised by e-commerce websites that compete with Google that they are being treated unfairly in search ranking, and in their ability to purchase search advertising.

"We also will continue to closely examine the impact of further acquisitions in this sector," Kohl said.

The Justice Department is currently reviewing Google’s proposed $700 million acquisition of flight information company ITA Software, a deal which is facing opposition from several leading online travel sites.

According to figures released on Friday by tracking firm comScore, Google remains the overwhelming leader of the US search market although its US market share slipped to 65.4 percent in February from 65.6 percent in January.

Apple’s iPad 2 Hits Stores

Apple’s new iPad goes on sale across the United States on Friday as the gadget-maker seeks to stay a step ahead of its rivals in the booming market for sleek touchscreen tablet computers.

Apple was to begin taking online orders for the iPad 2, which was unveiled by chief executive Steve Jobs last week, at 4:00 am (0900 GMT), but as of 5:00 am it did not yet appear to be available.

The device was to go on sale at the company’s 236 US stores starting at 5:00 pm (2200 GMT).

The iPad 2, which is one-third thinner, nearly 15 percent lighter and faster than the model released last April, will go on sale in another two dozen countries on March 25.

Besides the size and weight, the other major improvement to the new iPad is the addition of front- and rear-facing cameras that allow users to take still pictures and video and hold video conversations.

Apple sold 15 million iPads last year, bringing in $10 billion in new revenue and creating an entirely new category of consumer electronics devices.

Dozens of other companies have been scrambling since then to bring their own touchscreen tablets to market, most of them relying on Google’s Android software.

But with the exception of the Galaxy Tab from South Korea’s Samsung, rival tablet-makers have enjoyed little success.

Technology research firm Gartner is forecasting sales of 55 million tablet computers worldwide this year and another research firm, Forrester, said Apple has little to worry about for now.

"Competing tablets to the iPad are poised to fail, which is why we’re forecasting that Apple will have at least 80 percent share of the US consumer tablet market in 2011," Forrester said.

The iPad 2 has received mostly glowing reviews from the influential technology columnists of The Wall Street Journal and The New York Times.

"While it’s evolutionary rather than revolutionary like the first model, the changes Apple has made are generally pleasing and positive, and the device worked very well for me," the Journal’s Walter Mossberg said.

Mossberg said the iPad 2 "keeps Apple ahead in the tablet race, at least for now." But he was critical of the quality of the photos taken by its still cameras and its inability to play Adobe Flash video.

"This is a deliberate decision by Apple, and puts its devices at a disadvantage for some users when compared with Android tablets, which can play Flash, or say they will soon, albeit not always well," Mossberg said.

While pleased with the iPad 2 overall, Mossberg said it was not a must buy for owners of the old model.

"Unless you are desperate for the cameras or feel you are laboring under the greater bulk of the original model, I don’t advise that iPad owners race to get the new version," he said.

David Pogue of the Times said the improvement in thinness, weight and speed "transforms the experience" of using an iPad and the cameras are a "treat."

"The entire screen is your viewfinder," he said.

Pogue also noted the iPad 2’s inability to play Flash video but said the device "will still dominate the market, because it dominates in all the most important criteria: thinness, weight, integration, beauty - and apps."

More than 65,000 applications have been created for the iPad, while there are currently only about 100 crafted for tablets running Google’s Android operating system.

Pogue said another factor likely to keep Apple on top is the fact that the iPad 2 costs less than the Samsung Galaxy Tab and Motorola’s new Xoom.

Apple is selling the iPad 2 at the same prices as the original iPad, ranging from $499 for the basic 16-gigabyte version to $829 for the top-of-the-line 64-GB model.

The iPad 2 will be available on March 25 in Australia, Austria, Belgium, Britain, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden and Switzerland.

New Chrome Browser Ready for The World

Google on Tuesday released a finished version of its speedy new Chrome Web browsing software for desktop or laptop computers.

The latest version of Chrome promised quick and responsive handling of software running in the Web browser.

"We realize that speed isn’t just about pure brawn in the browser," Google engineer Tim Steele said in a blog post announcing the latest Chrome release.

"It’s also about saving time with simple interfaces."

Google improved settings for bookmarks, passwords, searches and home pages as well as enhanced protection from websites booby-trapped by hackers with malicious code.

The latest Chrome browser software is available free online at google.com/chrome. Earlier versions of the Web browser already being used in computers will be automatically updated, according to Google.

Microsoft’s Internet Explorer is the most widely used Web browser in the United States followed by Firefox, Chrome and Apple’s Safari.

Faster, More Secure IE 9 Set to Debut March 14

Just after proclaiming Internet Explorer 6 needs to die, Microsoft is readying the launch of IE9, the newest version of its market-leading web browser.

Microsoft plans to debut the browser at the SXSW (South by Southwest Conference and Festivals) conference in Austin on March 14, and the browser will be available for download that same evening.

IE 9 does what no Microsoft browser has done before -- embraces HTML 5. HTML 5 is the latest greatest version of HTML, the core coding language for the web. With HTML 5, rich media web sites with stronger animation are made possible.

One of the key new features in IE9 is Tracking Protection. This feature was originally planned for IE8, but Microsoft held off on executing the software that lets customers control tracking on web sites. Essentially, Tracking Protection lets consumers filter content in a page that may have an impact on their privacy.

Here’s how Tracking Protection works: Consumers can indicate what web sites they would prefer to not exchange information with. Consumers do this by adding Tracking Protection lists to IE. Anyone, and any organization, on the web can create and publish Tracking Protection lists.

In practice, this means that if you visit a news site, then a sports site, then some other web site, third-party advertisers can’t build a profile of browsing activity. Although there are many benefits to building those profiles, including driving more relevant, personalized content, Microsoft is responding to privacy concerns by giving consumers a way to block that tracking.

IE9 also offers InPrivate Browsing, another feature to help consumers control what their machine remembers about browsing sessions. InPrivate Filtering was a forerunner of Tracking Protection.

"This is Microsoft’s comeback platform. They’ve broken from the pack and the end result is that it’s incredibly fast," said Rob Enderle, principal analyst at The Enderle Group. "It’s probably one of the most secure products Microsoft has ever brought out."

Beyond speed, security and privacy features, Enderle said Microsoft has something else important in the realm of web browsers: massive developer support to use the underpinning features. That means there should be a number of web sites at launch that make unique use of some of the performance and graphics capabilities of the product.

"This is probably going to be one of Microsoft’s strongest launches ever and probably one of the most important IE launches since IE 3 when Microsoft stepped away from Spyglass," Enderle said. "So this is very critical one for Microsoft and one where the company is taking a pretty big risk by jumping out so far ahead of the other guys with regard to technology."

Will the advances be enough to ward off Firefox, Chrome, Opera and other competing browsers? It’s too soon to tell, but one thing is certain: Microsoft is focused on making IE 9 a success. And, Enderle said, when Microsoft focuses it’s hard for them to miss.

Twitter Must Give User Info in WikiLeaks Probe

A federal magistrate ruled Friday that prosecutors can demand Twitter account information of certain users in their criminal probe into the disclosure of classified documents on WikiLeaks.

Three of the five account holders targeted by the government had asked the judge to reverse an earlier order she issued requiring Twitter to turn over the information to prosecutors. The Twitter users argued that the government was on a fishing expedition and its request amounted to an unconstitutional violation of their freedom of speech and association.

But in a ruling issued Friday, U.S. Magistrate Judge Theresa Carroll Buchanan said the government’s request was reasonable and did nothing to hamper the Twitter users’ free speech rights.

"The freedom of association does not shield members from cooperating with legitimate government investigations," Buchanan wrote in her 20-page opinion.

The efforts by the Twitter users marked the first legal skirmish in the Justice Department’s criminal investigation of the WikiLeaks disclosures, but is unlikely to be the last. The Twitter users’ lawyers, including the American Civil Liberties Union and the Electronic Frontier Foundation - had previously said they would appeal an unfavorable ruling from the magistrate to a trial judge.

A federal law - the Stored Communications Act - allows prosecutors to obtain certain electronic data without a search warrant or a demonstration of probable cause. Instead, the government must only show that it has a reasonable belief that the records it seeks are relevant to an ongoing criminal investigation.

Prosecutors said the law is used routinely in criminal investigations, and that the WikiLeaks investigation is no different from any other criminal probe.

The U.S. Attorney’s office for the Eastern District of Virginia, which is investigating the WikiLeaks case, declined comment after Friday’s hearing.

Buchanan agreed with prosecutors, and said the Twitter users had no reason to expect that the information sought by prosecutors would be kept private. The order does not seek the content of the tweets themselves, which are already publicly disseminated. Instead, it seeks certain "non-content" information, like billing records and IP addresses associated with the accounts.

"The Twitter Order does not seek to control or direct the content of petitioners’ speech or association," Buchanan wrote.

Lawyers for the Twitter users had argued that people would be less likely to speak freely if they knew that doing so could result in their being subjected to a government investigation.

Twitter did not immediately respond Friday to questions about whether it now intends to turn over the information sought by prosecutors.

The original order issued by Buchanan in December 2010 at prosecutors’ request sought account information from Wikileaks founder Julian Assange and Pfc. Bradley Manning, who is being held at Quantico Marine Corps Base amid allegations that he leaked classified documents about the Iraq and Afghanistan wars to WikiLeaks.

Three other accounts belonging to American Jacob Appelbaum, Dutch citizen Rop Gonggrijp and Birgitta Jonsdottir, a member of Iceland’s parliament, were also targeted. Those three challenged the court order. Assange has contended that, as an Australian citizen, he is not subject to American law.

Buchanan also rejected a request that would have required the government to disclose whether it sought similar records from other social networking sites like Facebook.

IE6 Isn’t the Only Obsolete Browser In Use

With Microsoft’s push to eradicate its aging, problematic IE6 browser , PCMag looked into what other outdated surfing software people are still using. The array of Web browsers still in circulation would probably surprise the majority of Internet users, who by a large margin now browse with newer versions of IE, Firefox, Chrome, and Safari.

To conduct this investigation, we started PCMag.com’s own traffic analysis tools, Adobe Omniture SiteCatalyst, to see what unlikely software our readers were using, then checked out Internet-wide stats from Net Applications’ NetMarketShare.

First, let’s see where the leaders stand on PCMag.com. For all of 2011 up to the present moment, 28 percent of our readers used Firefox 3.6, followed closely by Internet Explorer 8, with 26 percent. A bigger gap separated the next app - Google Chrome 8, with 9.6 percent. Since the latest version of Chrome is 9, and the software updates automatically, I checked the first week of March, finding Chrome 9’s share up over 17 percent, with version 8 dropping all the way to 0.4 percent. That’s a great case for Google’s auto-update strategy, which would have saved Microsoft from its present IE6 predicament. But it didn’t save over 600 of our site visitors from using Chrome 1.0, and over twice that from using version 2.

By contrast, IE7 was still at 8 percent. Remember, that version came out over four years ago, in October 2006, and its performance on browser benchmarks is orders of magnitude slower than the current crop of browser versions. On PCMag.com, IE6 accounts for just 2.3 percent of the audience, while Omniture lists the Internet average at 4.6 percent, and Net Applications puts it at 11.3 percent for 2011 so far.

Older Firefox versions linger longer than those of Chrome, too. So far this year, 1.5 percent still use version 3.5, which was superceded by 3.6 over a year ago, in January 2010. But it doesn’t end there: we still have readers using versions 3, 2, and even 1. Maybe strangest of all, some readers were using /betas/ of old versions: over 500 readers used the beta of Firefox 3.0, and a dozen even used the beta of Firefox 1.5, which dates back to 2005.

Then we get to the more obscure browsers, which no longer even have current versions. We found over 35,000 readers used MSN Explorer, Microsoft’s discontinued browser cum e-mail and IM app. I was shocked to see that you could actually still download an ancient version of this obsolete browser, and the top result in a Bing search for the term "MSN Explorer" brings up a page offering a download of a version that includes Internet Explorer 5.5 - an even older app than the one Microsoft is trying to eradicate.

In another surprise from another era, we had over 20,000 people so far in 2011 using Netscape Navigator to browser our site. Oddly, more of them used version 2.0 - over 10,000 - while nearly 7,000 used version 4, and almost 5,000 used version 3. Over 1,000 of our site visitors used either version 1.1 or 1.2. Clearly, for some, this is still the age of the dawn of the Web. We were only surprised that no one was using Mosaic, the first popular browser.

Perhaps the oddest browser used was Nutscrape 1.0, which Omniture reported for four site visitors in 2011. Probably just some hacker’s joke, we could only find that it may have run on the pre-PC CP/M operating system. Though that OS didn’t show up in our traffic analysis, some surprisingly outdated ones did - we had 3,067 visitors who used Windows 98, 1,663 ran Windows Me, and 282 were running Window 3.x. Non-Windows blasts from the past were also represented: 438 used the ill-fated OS/2 operating system, and five ran Amiga OS.

So while Microsoft’s campaign to eradicate Internet Explorer 6 is laudable, it seems clear that there’s nothing anyone can to do stop people from running some seriously outdated software.

German Foreign Office Kills Desktop Linux, Hugs Windows XP

Openistas beware! Politicos at the German Foreign Office are reportedly ditching Linux in favour of returning their desktop PCs to Windows XP-based systems.

According to a report on netzpolitik.org, which was diligently spotted by The H, the German Foreign Office recently decided to dump their Linux-based machines.

That move came despite the office being reassured in two separate appraisals carried out by consulting outfit McKinsey that Linux and open source software formed a perfectly adequate part of the German Foreign Office’s IT strategy.

McKinsey did highlight some areas of concern during its first study of the FOSS strategy in 2009, but concluded that it "could generally be considered sound".

Somewhat surprisingly, one problem highlighted by McKinsey was interoperability with some office documents. But it was clearly noted that a simple update on all Linux desktops to the latest versions of OpenOffice could fix that particular issue.

A second study last year by the consultancy group found that a shift to a pure Windows environment on the German Foreign Office’s desktop computers would be costly and work-intensive.

But by the end of last year the FO’s IT commissioner Dr Michael Groß told ministry staff that a decision had been reached in August 2010 to revert the entire desktop estate back to Windows XP due to "massive user criticism" about "unsolved interoperability problems".

And in case you’re wondering why the migration didn’t move directly to Microsoft’s latest operating system, Groß said that Windows XP, which turns 10 later this year, was the "uniform basis for the actual step towards implementing a new system using Windows 7 and Office 2010".

Questions have been raised in Germany’s Bundestag parliament about the sudden switch back to Windows XP.

The German government claimed the OS shake-up wouldn’t lead to it having to foot the bill for "indirect costs", and retorted that the migration to "standardised software products" was likely to result in "efficiency gains".

All that despite McKinsey confirming in 2009 that the German Foreign Office had splurged less cash on its individual IT workspaces then any other federal authority in the country while running a Linux desktop shop. Shurely shome mishtake? fi

To LOL, Or Not LOL? That Is The Question

There was a time when LOL - "laughing out loud" - was so simple.

If I thought something in a casual online conversation was funny, I typed it. If I wanted to let someone know I was kidding in an e-mail or an instant message, same.

I might’ve even felt a little cool, using inside lingo that, at one time, was exclusive to the online world. (You know I’m not the only one who thought so.)

Today, though, I’m sensing a shift, even in my own thoughts about LOL. Certainly, it’s as ubiquitous as ever. Just search for it on Twitter or Facebook to see how often people use it. Not exactly deep and meaningful stuff, mind you, but there sure is a lot of it.

Perhaps that’s why, at least in some circles, LOL has lost its cachet. And at its worst, it’s making people a little cranky.

It’s overused and meaningless, they say. It "epitomizes lazy, and makes people a liar" says Seth Ginsburg, a 29-year-old New Yorker. "Are they really laughing out loud?"

Comedian Demetri Martin has joked that he uses "LTMQ - laughing to myself quietly."

"It’s more honest," he says.

I laugh every time I hear that joke - out loud, no less - because I too have this internal debate: I tell myself that I’ll only type LOL if I’m really "LOL-ing."

But I fail, regularly. It’s just too easy to type (two keys, one finger or a thumb, if it’s a cell phone), too convenient a response.

Sure, there are LOL haters out there, seemingly more all the time. But for better or worse, this modern-day acronym has become ingrained in our lexicon and, for some, has evolved in meaning.

"It’s brevity at its finest, and it gets a point across," says 25-year-old Arzi Rachman, another New Yorker.

Try as some might, LOL will not be easily shaken.

The exact origins of this three-letter acronym, in its current form, are not easy to pin down. Most likely, it was a gamer or hacker who first used LOL (or "lol") on an electronic message board, probably sometime in the 1980s.

Its use became more common on early Internet services such as CompuServe and Netcom. By the mid-1990s, when even more people joined America Online, the term LOL hit the mainstream in chat rooms and in instant messaging.

It morphed, as well. If you thought something was really, really funny, for instance, you might type ROFL - "rolling on the floor laughing" - or LMAO - "laughing my (you know what) off."

By 2004, fatigue was setting in. LOL was added to the "List of Words to Be Banished from the Queen’s English for Mis-use, Over-use and General Uselessness," updated each year at Lake Superior State University in Michigan.

Regardless, LOL went forth and multiplied and has since seeped into spoken language.

"At times, I do say LOL," says Rachman, a college student, "usually to accentuate sarcasm, or something along those lines."

Of course, when speaking of text conversations, one can’t forget the sideways smiley - :-) - which you might call LOL’s older cousin.

Scott Fahlman, a research professor in the computer science department at Carnegie Mellon University, often gets the credit for first suggesting that emoticon nearly 30 years ago. His fellow academics quickly embraced it and ushered in its everyday online use.

The sideways smiley has gotten bashed too -- it’s been called the equivalent of "i’s" dotted with hearts.

But asked if he’s ever used LOL, Fahlman will tell you, "Nope." He draws the line.

"It sort of strikes me as kind of - this is going to sound sexist - a teenage girl thing," he says, "a high school thing."

But is that really true? Does the use of LOL really fall along generational lines? Was the implication that some of us are too old to use LOL?

"One of the things that’s pretty clear - whether LOL is in or passe - it depends on your social circle," says Naomi Baron, a linguist at American University who wrote the book "Always On: Language in an Online and Mobile World."

As more people of all ages forge online lives, those social circles may be less divided by generation, though not completely.

In surveying college students about their use of online or texted terms, for example, Baron has noticed a difference in the way they use LOL. For them, it is often used as a simple acknowledgment that may have nothing to do with laughter. Instead, LOL might mean "oh," "got it," "heard you" or "really?"

That use might bother some people; Baron also has colleagues who scold her when she doesn’t correct students who greet her with a "hey!"

But she says that kind of evolution in language happens all the time. Sometimes, it’s for practical reasons or convenience. Other times, it’s simply a style or trend.

In the 18th and early 19th centuries in England, Baron notes, it was commonplace to sign a letter using "Yr Hum Serv," an abbreviation for "Your Humble Servant."

"Everybody knew what that meant," she says. "It was just convention."

Today, it’s happening on Twitter with "hash tags" - the number symbol. Originally meant to mark terms or events that users may search for, people have started using hash tags to highlight the equivalent of a funny or snarky side comment. That use has since transferred to Facebook, where hash tags don’t even apply.

"It’s all part of marking your territory," Baron says. "People mark it linguistically. They mark it by dress. They mark it by how many earrings they have in their ears - you name it."

All of that makes sense to Ben Huh, who heads the Seattle-based company that oversees popular humor websites such as "I Can Has Cheezburger?" and "FAIL Blog." His sites allow users to share funny videos and photos, which he and his staff call "LOLs" or "lolz."

"I don’t actually remember the first time I started using this lingo because it seemed to me that it was just part of life," says Huh, who is 33. "I didn’t adopt the use of Internet cultural languages. I just grew up with it."

So for him, using LOL feels as natural as saying "OK," or "cool." He also couldn’t care less if a person who uses LOL isn’t really laughing out loud.

"It’s like the suburban dad who wants to put his hat on backward," he says, "versus the kid who puts a hat on backward because that’s just what they do."

It’s not necessarily a matter of age, he says, but whether it’s really just who you are.

I’ve decided that LOL is me, sometimes.

Just like I don’t send text messages to my mother, because they’d never see the light of day, I probably wouldn’t use LOL with my boss or an acquaintance or any number of people who kvetched about LOL when I told them I was writing a story about it.

They’re more likely to see the buttoned-up purist in me who avoids cliches "like the plague," as one of my college professors once encouraged me to do.

But then there’s the me who has the urge to wear my pajamas to the coffee shop on a lazy Sunday morning.

She uses LOL - and wishes the world would lighten up, just a little.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.